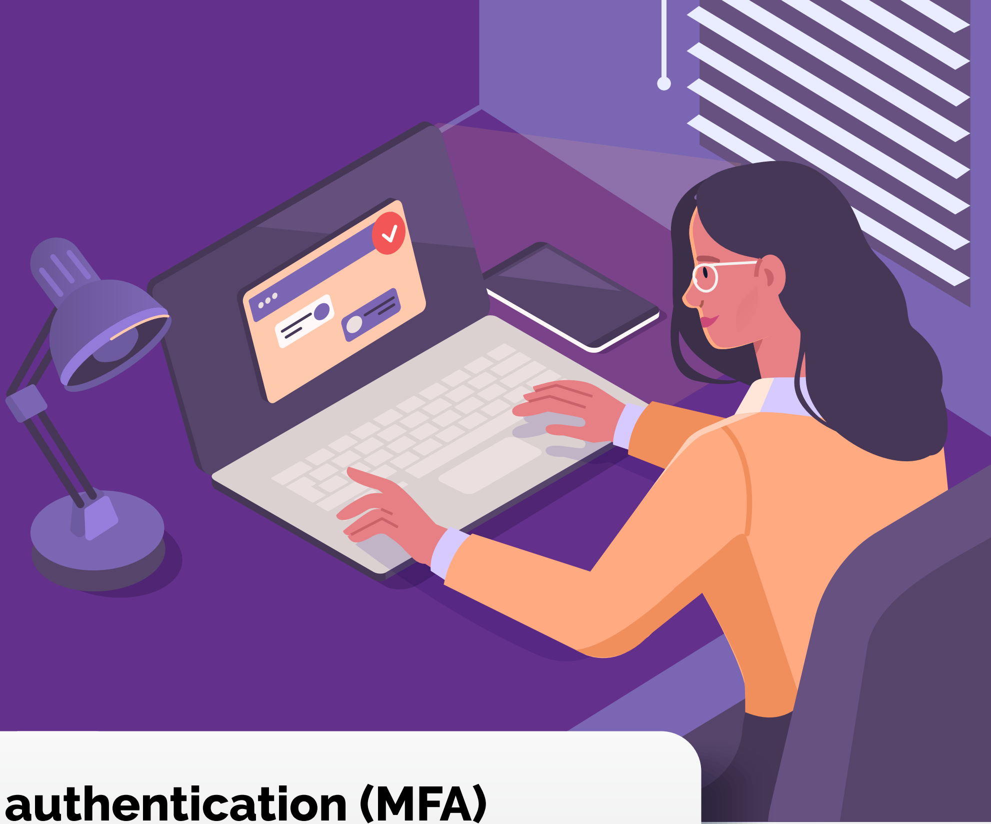
5 Hybrid Workforce Cybersecurity Safety Tips

Are you ready to transition your clients back to the office? Adopting a hybrid work model is here to stay. It's important to remember that home networks are generally less secure than business networks, which gives cybercriminals an opportunity to strike. Here are five tips to protect your business from the cybersecurity pitfalls of supporting a hybrid workforce.



01 Use multifactor authentication (MFA)

If your budget is limited, MFA gives you the most bang for your buck because this single tool stops up to 99% of cybercrime in its tracks.

02 Reduce cyberattack risk with automated email security

Employees can't fall for phishing emails they don't see. In fact, traditional security or SEGs fail to prevent 47% of all phishing messages.

03 Encourage regular breaks to recharge

Employees are over 40% more likely to make mistakes that lead to cybersecurity incidents when they're stressed, tired or distracted, even while working remotely.

04 Make it easy to ask for help with suspicious emails

Make it easy to report dodgy messages or get safety advice since 90% of incidents that end in a data breach start with a phishing email.

05 Don't slack on security awareness training

Companies that engage in security awareness training for all employees at least quarterly, experience up to 70% fewer cybersecurity incidents.

The new datapoints above are linked for specific attribution if desired but all data has been reported in the ID Agent blog Inside the Ink in 2020-2021.

ID AGENT
A Kaseya COMPANY